IT Security at the Regents Institutions

Target says up to 70 million more customers were hit by December data breach

Target Offers $10 Million Settlement In Data Breach Lawsuit

US | Fri May 15, 2015 2:36pm EDT

Cyberattack on Penn State college said to have come from China

BY DEVIKA KRISHNA KUMAR

REUTERS

Pennsylvania State University said on Friday that two cyberattacks at its College of Engineering, including one in 2012 that originated in China, compromised servers containing information on about 18,000 people.

Related: U.S., TECH, C

HOME | POLICY | FINANCE

IRS reports security breach

COMMENTS 14

By Bernie Becker - 03/18/14 03:57 PM EDT

Thousands of IRS employees had their personal information put at risk when an agency staffer brought home an unencrypted thumb drive, the agency said in a statement on Tuesday.
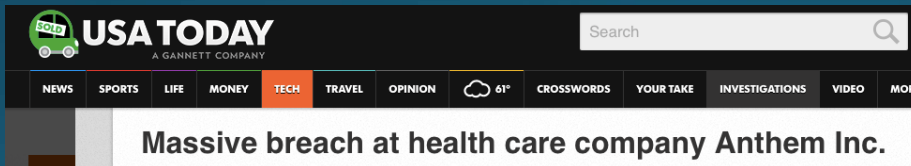
TECHNOLOGY

Cyberattack Exposes I.R.S. Tax Returns

By JADA F. SMITH   MAY 26, 2015

Anthem

Technology | Tue Feb 24, 2015 4:29pm EST

Related: TECH

Anthem says at least 8.8 million non-customers could be victims in data hack

THE HOME DEPOT

USA TODAY
A GANNETT COMPANY

Search

NEWS   SPORTS   LIFE   MONEY   TECH   TRAVEL   OPINION   ☁ 61°   CROSSWORDS   YOUR TAKE   INVESTIGATIONS   VIDEO   MORE

Massive breach at health care company Anthem Inc.

SONY

TECH

Home Depot Hackers Exposed 53 Million Email Addresses

Hackers Used Password Stolen From Vendor to Gain Access to Retailer's Systems

Massive Security Breach At Sony -- Here's What You Need To Know

Common IT Security Threats

- Control of IT accounts
- Control of IT systems & resources
- Data theft or corruption
- Equipment theft
- Disable/destroy network or systems

- Many methods of attack
- Constantly evolving
- Increasingly targeting the human element
- Everyone has a role in security

Collaborative Activities

- BORIS (Board of Regents Information Security)
- CIO Council
  - Weekly video conference call
  - Security sub-group
- Joint meeting
  - 10-15 personnel from each school
  - 7-10 technical areas
  - Joint projects, joint purchases, common solutions, & best practices

IOWA STATE UNIVERSITY

Security Road Map
April 2014

1. Identify and protect storage reserves that contain restricted university data;

2. Review and improve business processes;

3. Encrypt all university-owned laptops;

4. Implement stronger password policies;

5. Scan campus systems for known security vulnerabilities; and,

6. Increase and improve educational resources for students, staff, and faculty members.

IOWA STATE UNIVERSITY

Security Focus

- **Data Classification Policy & Encryption**

- **Education**
  - Multimedia focused with videos and news media
  - Intermediate level videos & policy education
  - Advanced certification & continuing education

- **Examination**
  - Vulnerability scanning & remediation
  - ISEAGE partnership & Information Assurance Center
  - Internal & external assessments of systems & controls – implement best industry practices

- **Enhancements**
  - Investment & collaboration among colleges, research centers, & central IT
  - Collaboration among world-class technology faculty researchers

Security Framework & Approach

- Based on National Cybersecurity & Compliance Standards

- Safeguards Throughout Systems Lifecycle

- Layered Approach

- Campus Community Engagement & Commitment
  - UNI Security Working Group
  - Technical Forums
  - Collaborations & Memberships
  - Policies, Guidelines, & Best Practices

University of Northern Iowa

Security Initiatives

- Reduction of Sensitive Information
- Examination of Business Processes & Access Rights
- Multifactor Authentication
- Encryption
- System Hardening Standards
- Security Reviews
- IT Security Department
- Security Awareness Training

University of Northern Iowa

Foundational Elements

- Dedicated IT security team
- Centralized account management & multifactor authentication
- User awareness & training
- Robust security policies
- Technical measures
- Reduced sensitive data footprint & safeguarding of institutional data

Continuing Initiatives

- Mobile device encryption

- Additional use of multifactor authentication

- New version of online security awareness training

- Using the TIER process as an opportunity to review security

Discussion